SEC. ___. EXPANDING THE FUNDING AUTHORITY FOR RENOVATING, CONSTRUCTING, AND EXPANDING CERTAIN FACILITIES.

Section 509 of the Indian Health Care Improvement Act (25 U.S.C. 1659) is amended—

(1) by striking ''minor'' before ''renovations''; and

(2) by striking '', to assist'' and all that follows through ''standards''.

SA 2134. Mr. KING (for himself, Mr. SASSE, and Mr. ROUNDS) submitted an amendment intended to be proposed by him to the bill H.R. 3684, to authorize funds for Federal-aid highways, highway safety programs, and transit programs, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title VI of division G, add the following:

Subtitle C—National Cyber Resilience Assistance Fund

SEC. 70621. ESTABLISHMENT OF THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) the United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the United States Government nor the private sector alone is currently equipped to provide;

(2) the United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to the disadvantage of the United States, and at little cost to themselves;

(3) this new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem;

(4) reducing the vulnerabilities adversaries can target denies them opportunities to attack the interests of the United States through cyberspace;

(5) the public and private sectors struggle to coordinate cyber defenses, leaving gaps that decrease national resilience and create systemic risk;

(6) new technology continues to emerge that further compounds these challenges;

(7) while the Homeland Security Grant Program and resourcing for national preparedness under the Federal Emergency Management Agency are well-established, the United States Government has no equivalent for cybersecurity preparation or prevention;

(8) the lack of a consistent, resourced fund for investing in resilience in key areas inhibits the United States Government from conveying its understanding of risk into strategy, planning, and action in furtherance of core objectives for the security and resilience of critical infrastructure;

(9) the Federal Government must fundamentally shift the way it invests in resilience and shift the focus away from reactive disaster spending towards research-supported and risk-driven proactive investment in critical infrastructure cyber resilience;

(10) Congress has worked diligently to establish the Cybersecurity and Infrastructure Security Agency, creating a new agency that can leverage broad authorities to receive and share information, provide technical assistance to operators, and partner with stakeholders across the executive branch, State and local communities, and the private sector;

(11) the Cybersecurity and Infrastructure Security Agency requires strengthening in its mission to ensure the national resilience of critical infrastructure, promote a more secure cyber ecosystem, and serve as the central coordinating element to support and integrate Federal, State, local, and private-sector cybersecurity efforts; and

(12) the Cybersecurity and Infrastructure Security Agency requires further resource investment and clear authorities to realize its full potential.

(b) AMENDMENTS.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2202(c) (6 U.S.C. 652(c))—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in the first paragraph designated as paragraph (12), relating to the Cybersecurity State Coordinator—

(i) by striking ''section 2215'' and inserting ''section 2217''; and

(ii) by striking ''and'' at the end; and

(C) by redesignating the second and third paragraphs designated as paragraph (12) as paragraphs (13) and (14), respectively;

(2) by redesignating section 2218, as added by section 70612 of this Act, as section 2220A;

(3) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(4) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(5) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(6) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

(7) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216; and

(8) by adding at the end the following:

''SEC. 2220B. NATIONAL CYBER RESILIENCE ASSISTANCE FUND.

''(a) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given that term in section 2209.

''(2) ELIGIBLE ENTITY.—The term 'eligible entity' means an entity that meets the guidelines and requirements for eligible entities established by the Secretary under subsection (d)(4).

''(3) FUND.—The term 'Fund' means the National Cyber Resilience Assistance Fund established under subsection (c).

''(4) NATIONAL CRITICAL FUNCTIONS.—The term 'national critical functions' means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

''(b) CREATION OF A CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY AND A NATIONAL RISK MANAGEMENT CYCLE.—

''(1) INITIAL RISK IDENTIFICATION AND ASSESSMENT.—

''(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, vulnerabilities, and consequences.

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with Sector Risk Management Agencies, critical infrastructure owners and operators, and the National Cyber Director.

''(C) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A).

''(D) REPORT.—Not later than 1 year after the date of enactment of this section, the Secretary shall submit to the President, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the risks identified by the process established under subparagraph (A).

''(2) INITIAL NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers the report required under paragraph (1)(D), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—In the strategy delivered under subparagraph (A), the President shall—

''(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise, disrupt, or impede the ability of the critical infrastructure to support the national critical functions of national security, economic security, or public health and safety;

''(ii) identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified;

''(iii) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each;

''(iv) outline the budget plan required to provide sufficient resources to successfully execute the full range of activities proposed or described by the strategy; and

''(v) request any additional authorities or resources necessary to successfully execute the strategy.

''(C) FORM.—The strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers the strategy under subparagraph (A), and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate congressional committees on the national risk management cycle activities undertaken pursuant to the strategy.

''(4) FIVE YEAR RISK MANAGEMENT CYCLE.—

''(A) RISK IDENTIFICATION AND ASSESSMENT.—Under procedures established by the Secretary, the Secretary shall repeat the conducting and reporting of the risk identification and assessment required under paragraph (1), in accordance with the requirements in paragraph (1), every 5 years.

''(B) STRATEGY.—Under procedures established by the President, the President shall repeat the preparation and delivery of the critical infrastructure resilience strategy required under paragraph (2), in accordance with the requirements in paragraph (2), every 5 years, which shall also include assessing the implementation of the previous national critical infrastructure resilience strategy.

''(c) ESTABLISHMENT OF THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.—There is established in the Treasury of the United States a fund, to be known as the 'National Cyber Resilience Assistance Fund', which shall be available for the cost of risk-based grant programs focused on systematically increasing the resilience of public and private critical infrastructure against cybersecurity risk, thereby increasing the overall resilience of the United States.

''(d) ADMINISTRATION OF GRANTS FROM THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.—

''(1) IN GENERAL.—In accordance with this section, the Secretary, acting through the Administrator of the Federal Emergency Management Agency and the Director, shall develop and administer processes to—

''(A) establish focused grant programs to address identified areas of cybersecurity risk to, and bolster the resilience of, critical infrastructure;

''(B) accept and evaluate applications for each such grant program;

''(C) award grants under each such grant program; and

''(D) disburse amounts from the Fund.

''(2) ESTABLISHMENT OF RISK-FOCUSED GRANT PROGRAMS.—

''(A) ESTABLISHMENT.—

''(i) IN GENERAL.—The Secretary, acting through the Director and the Administrator of the Federal Emergency Management Agency, may establish not less than 1 grant program focused on mitigating an identified category of cybersecurity risk identified under the national risk management cycle and critical infrastructure resilience strategy under subsection (b) in order to bolster the resilience of critical infrastructure within the United States.

''(ii) SELECTION OF FOCUS AREA.—Before selecting a focus area for a grant program pursuant to this subparagraph, the Director shall ensure—

''(I) there is a clearly-defined cybersecurity risk identified through the national risk management cycle and critical infrastructure resilience strategy under subsection (b) to be mitigated;

''(II) market forces do not provide sufficient private-sector incentives to mitigate the risk without Government investment; and

''(III) there is clear Federal need, role, and responsibility to mitigate the risk in order to bolster the resilience of critical infrastructure.

''(B) FUNDING.—

''(i) RECOMMENDATION.—Beginning in the first fiscal year following the establishment of the Fund and each fiscal year thereafter, the Director shall—

''(I) assess the funds available in the Fund for the fiscal year; and

''(II) recommend to the Secretary the total amount to be made available from the Fund under each grant program established under this subsection.

''(ii) ALLOCATION.—After considering the recommendations made by the Director under clause (i) for a fiscal year, the Director shall allocate amounts from the Fund to each active grant program established under this subsection for the fiscal year.

''(3) USE OF FUNDS.—

''(A) IN GENERAL.—Amounts in the Fund shall be used to proactively mitigate risks identified through the national risk management cycle and critical infrastructure resilience strategy under subsection (b) before cyber incidents occur, through activities such as—

''(i) proactive vulnerability assessments and mitigation;

''(ii) defrayal of costs to invest in backup systems critical to mitigating national or economic security risks, as determined by the Federal Government, with cost-sharing from the recipient entity in accordance with subparagraph (B);

''(iii) defrayal of costs to invest in replacing vulnerable systems and assets critical to mitigating national or economic security risks, as determined by the Federal Government, with more secure alternatives with cost-sharing from the recipient entity in accordance with subparagraph (B);

''(iv) grants to nonprofit entities to develop publicly available low-cost or no-cost cybersecurity tools for small-sized and medium-sized entities;

''(v) proactive threat detection and hunting; and

''(vi) network protections.

''(B) FEDERAL SHARE.—The Federal share of the cost of an activity described in clause (ii) or (iii) of subparagraph (A) carried out using funds made available under this section may not exceed—

''(i) for fiscal year 2022, 90 percent;

''(ii) for fiscal year 2023, 80 percent;

''(iii) for fiscal year 2024, 70 percent;

''(iv) for fiscal year 2025, 60 percent; and

''(v) for fiscal year 2026, and each fiscal year thereafter, 50 percent.

''(4) ELIGIBLE ENTITIES.—

''(A) GUIDELINES AND REQUIREMENTS.—

''(i) IN GENERAL.—In accordance with clause (ii), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a set of guidelines and requirements for determining the entities that are eligible entities.

''(ii) DEADLINES.—The Secretary shall submit the guidelines and requirements under clause (i)—

''(I) not later than 180 days after the date of enactment of this section, and every 2 years thereafter; and

''(II) not later than 90 days before the date on which the Secretary implements the guidelines and requirements.

''(B) CONSIDERATIONS.—In developing guidelines and requirements for eligible entities under subparagraph (A), the Secretary shall consider—

''(i) number of employees;

''(ii) annual revenue;

''(iii) existing entity cybersecurity spending;

''(iv) current cyber risk assessments, including credible threats, vulnerabilities, and consequences; and

''(v) entity capacity to invest in mitigating cybersecurity risk absent assistance from the Federal Government.

''(5) LIMITATION.—For any fiscal year, an eligible entity may not receive more than 1 grant from each grant program established under this subsection.

''(6) GRANT PROCESSES.—The Secretary, acting through the Administrator of the Federal Emergency Management Agency, shall require the submission of such information as the Secretary determines is necessary to—

''(A) evaluate a grant application against the criteria established under this section;

''(B) disburse grant funds;

''(C) provide oversight of disbursed grant funds; and

''(D) evaluate the effectiveness of the funded project in increasing the overall resilience of the United States with respect to cybersecurity risks.

''(7) GRANT CRITERIA.—For each grant program established under this subsection, the Director, in coordination with the Administrator of the Federal Emergency Management Agency, shall develop and publish criteria for evaluating applications for funding, which shall include—

''(A) whether the application identifies a clearly-defined cybersecurity risk;

''(B) whether the cybersecurity risk identified in the grant application poses a substantial threat to critical infrastructure;

''(C) whether the application identifies a program or project clearly designed to mitigate a cybersecurity risk;

''(D) the potential consequences of leaving the identified cybersecurity risk unmitigated, including the potential impact to the critical functions and overall resilience of the nation; and

''(E) other appropriate factors identified by the Director.

''(8) EVALUATION OF GRANTS APPLICATIONS.—

''(A) IN GENERAL.—Utilizing the criteria established under paragraph (7), the Director, in coordination with the Administrator of the Federal Emergency Management Agency, shall evaluate grant applications made under each grant program established under this subsection.

''(B) RECOMMENDATION.—Following the evaluations required under subparagraph (A), the Director shall recommend to the Secretary applications for approval, including the amount of funding recommended for each such approval.

''(9) AWARD OF GRANT FUNDING.—The Secretary shall—

''(A) review the recommendations of the Director prepared pursuant to paragraph (8); and

''(B) provide a final determination of grant awards to the Administrator of the Federal Emergency Management Agency to be disbursed and administered under the process established under paragraph (6).

''(e) EVALUATION OF GRANT PROGRAMS UTILIZING THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.—

''(1) EVALUATION.—The Secretary shall establish a process to evaluate the effectiveness and efficiency of grants distributed under this section and develop appropriate updates, as needed, to the grant programs.

''(2) ANNUAL REPORT.—Not later than 180 days after the conclusion of the first fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a report detailing the grants awarded from the Fund, the status of projects undertaken with the grant funds, any planned changes to the disbursement methodology of the Fund, measurements of success, and total outlays from the Fund.

''(3) GRANT PROGRAM REVIEW.—

''(A) ANNUAL ASSESSMENT.—Before the start of the second fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Director shall assess the grant programs established under this section and determine—

''(i) for the coming fiscal year—

''(I) whether new grant programs with additional focus areas should be created;

''(II) whether any existing grant program should be discontinued; and

''(III) whether the scope of any existing grant program should be modified; and

''(ii) the success of the grant programs in the prior fiscal year.

''(B) SUBMISSION TO CONGRESS.—Not later than 90 days before the start of the second fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives the assessment conducted pursuant to subparagraph (A) and any planned alterations to the grant program for the coming fiscal year.

''(f) LIMITATION ON USE OF GRANT FUNDS.—Funds awarded pursuant to this section—

''(1) shall supplement and not supplant State or local funds or, as applicable, funds supplied by the Bureau of Indian Affairs; and

''(2) may not be used—

''(A) to provide any Federal cost-sharing contribution on behalf of a State or local government;

''(B) to pay a ransom;

''(C) by or for a non-United States entity; or

''(D) for any recreational or social purpose.

''(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $75,000,000 for each of fiscal years 2022 through 2026.

''(h) TRANSFERS AUTHORIZED.—During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to subsection (g) or other amounts appropriated to carry out the National Cyber Resilience Assistance Fund for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this section.

''(i) GOVERNMENT ACCOUNTABILITY OFFICE REPORT.—Not later than 1 year after the date of the enactment of this section, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs in the Senate and the Committee on Homeland Security in the House of Representatives a report containing the results of a study regarding the effectiveness of the programs described in this section.''.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by striking the item relating to section 2214 and all that follows through the item relating to section 2218, as added by section 70612 of this Act, and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity education and training programs.
''Sec. 2220A. State and Local Cybersecurity Grant Program.
''Sec. 2220B. National Cyber Resilience Assistance Fund.''.

(2) ADDITIONAL TECHNICAL AMENDMENT.—

(A) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

(B) EFFECTIVE DATE.—The amendment made by subparagraph (A) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

SA 2135. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill H.R. 3684, to authorize funds for Federal-aid highways, highway safety programs, and transit programs, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. ASSESSMENT AND ANALYSIS REGARDING THE EFFECT OF THE DIGITAL ECONOMY ON THE ECONOMY OF THE UNITED STATES.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate;

(B) the Committee on Environment and Public Works of the Senate;

(C) the Committee on Small Business and Entrepreneurship of the Senate;

(D) the Committee on Energy and Commerce of the House of Representatives;

(E) the Committee on Transportation and Infrastructure of the House of Representatives; and

(F) the Committee on Small Business of the House of Representatives.

(2) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary of Commerce for Communications and Information.

(3) BROADBAND.—The term ''broadband'' means an Internet Protocol-based transmission service that enables users to send and receive voice, video, data, or graphics, or a combination of those items.

(4) DIGITAL ECONOMY.—

(A) IN GENERAL.—Subject to subparagraph (B), the term ''digital economy'' has the meaning given the term by the Secretary in carrying out this section.

(B) CONSIDERATIONS.—In establishing a definition for the term ''digital economy'' under subparagraph (A), the Secretary shall consider—

(i) the digital-enabling infrastructure that a computer network needs to exist and operate; and

(ii) the roles of e-commerce and digital media.

(5) DIGITAL MEDIA.—The term ''digital media'' means the content that participants in e-commerce create and access.

(6) E-COMMERCE.—The term ''e-commerce'' means the digital transactions that take place using the infrastructure described in paragraph (4)(B)(i).

(7) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(b) BIENNIAL ASSESSMENT AND ANALYSIS REQUIRED.—Not later than 2 years after the date of enactment of this Act, and biennially thereafter, the Secretary, in consultation with the Director of the Bureau of Economic Analysis of the Department of Commerce and the Assistant Secretary, shall conduct an assessment and analysis regarding the contribution of the digital economy to the economy of the United States.

(c) CONSIDERATIONS AND CONSULTATION.—In conducting each assessment and analysis required under subsection (b), the Secretary shall—

(1) consider the impact of—

(A) the deployment and adoption of—

(i) digital-enabling infrastructure; and

(ii) broadband;

(B) e-commerce and platform-enabled peer-to-peer commerce; and

(C) the production and consumption of digital media, including free media; and

(2) consult with—

(A) the heads of any agencies and offices of the Federal Government as the Secretary considers appropriate, including the Secretary of Agriculture, the Commissioner of the Bureau of Labor Statistics, the Administrator of the Small Business Administration, and the Federal Communications Commission;

(B) representatives of the business community, including rural and urban internet service providers and telecommunications infrastructure providers;

(C) representatives from State, local, and tribal government agencies; and

(D) representatives from consumer and community organizations.

(d) REPORT.—The Secretary shall submit to the appropriate committees of Congress a report regarding the findings of the Secretary with respect to each assessment and analysis conducted under subsection (b).

SA 2136. Mr. SCHATZ submitted an amendment intended to be proposed by him to the bill H.R. 3684, to authorize funds for Federal-aid highways, highway safety programs, and transit programs, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in division [____], insert the following;

SEC. ____. CDBG DISASTER RECOVERY.

(a) Short Title.—This section may be cited as the ''Reforming Disaster Recovery Act''.

(b) Findings.—Congress finds that—

(1) following a major disaster declared by the President under section 401 or the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170), the subset or communities that are most impacted and distressed as a result or the disaster face critical social, economic, and environmental obstacles to recovery, including insufficient public and private resources to address disaster-related housing and community development needs for lower income households and distressed communities;

(2) unmet disaster recovery needs, including housing assistance needs, can be especially widespread among persons with extremely low, low, and moderate incomes;

(3) economic, social, and housing hardships that affect communities before disasters arc exacerbated during crises and can delay and complicate long-term recovery. especially after catastrophic major disasters;

(4) States, units of local government, and Indian Tribes within the most impacted and distressed areas resulting from major disasters benefit from flexibility to design programs that meet local needs, but face inadequate financial, technical, and staffing capacity to plan and carry out sustained recovery, restoration, and mitigation activities;

(5) the speed and effectiveness considerations of long-term recovery from catastrophic major disasters is improved by predictable investments that support disaster relief, long-term recovery, restoration of housing and infrastructure, and economic revitalization, primarily for the benefit of low- and moderate-income persons;

(6) undertaking activities that mitigate the effects of future natural disasters and extreme weather and increase the stock of affordable housing, including affordable rental housing, as part or long-term recovery can significantly reduce future fiscal and social costs, especially within high-risk areas, and can help to address outstanding housing and community development needs by creating jobs and providing other economic and social benefits within communities that further promote recovery and resilience; and

(7) the general welfare and security of the nation and the health and living standards of its people require targeted resources to support State and local governments in carrying out their responsibilities in disaster recovery and mitigation through interim and long-term housing and community development activities that primarily benefit persons of low and moderate income.

(c) Definitions.—In this section;

(1) DEPARTMENT.—The term ''Department'' means the Department of Housing and Urban Development.